International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1123

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Differentiated security service for secure mobile end-to-end data communication

Recommendation ITU-T X.1123

ITU-T

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1123

Differentiated security service for secure mobile end-to-end data communication

Summary

Recommendation ITU-T X.1123 describes the differentiated security service for secure mobile communication. The investigation of differentiated security service is important for both service providers and users. The service providers can use the differentiated security service to overcome the rigorous circumstances of wireless access networks and satisfy various users and services with different levels of security. The differentiated security service is realized by security policy with three layers. One layer is super security policy used as a value-added service that safeguards mobile communication with sensitive information. The second layer is baseline security policy used as the prevalent service that satisfies mobile communication without sensitive information. The last layer is no security policy, defined as the policy under which no security function is configured during communication.

Source

Recommendation ITU-T X.1123 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

Differentiated, security dimension, security level, security policy, security service.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Introduction

It is necessary to establish a differentiated security service in secure mobile communication. The reasons are described as follows:

- *Rigorous mobile environment*

  The number of types of services that are provided through mobile networks is increasing quickly. Moreover, the number of mobile users also grows remarkably all around the world. Similar to wired networks, mobile networks are also threatened by various attacks. In addition, the mobile environment has many limitations such as limited computing power in mobile terminals, inadequate memory space and low network bandwidth at the air interface. Therefore, the running of applications is more difficult in mobile networks than that in wired networks. Since the purpose of a security service is to organize various security technologies together to achieve a certain level of security for various applications, a differentiated security service mechanism is necessary for applications in the rigorous mobile environment.

- *Additional investment for security*

  Compared with unsecured networks, secure networks require additional investment from the service provider's point of view. Moreover, there is no absolute network security. The investment in security strongly relies on the level of security the network can provide. The additional investment at least includes network management of security, security devices, additional consumption on bandwidth and computing power, training for security managers and users, etc.

  When telecommunication networks evolve from circuit switched to packet switched, multimedia communication develops fast. The data volume of multimedia communication is much larger than that of audio communication. Data protection with a unique high security level becomes impossible because of the large, real-time data flow. For example, in second generation mobile networks, such as the GSM network, we can encrypt all the data flow at the air interface since the audio communication has a much smaller data flow compared with multimedia communication. However, in third generation mobile networks, when multimedia communication is popular, we need differentiated security levels to protect data flow and save resources.

  Since next generation networks are based on package networks, the open characteristics of package networks will cause many new security threats. The intelligence of mobile terminals also induces various threats from viruses. Thus, simple management is necessary to integrate the essential configuration of security for users.

  Evidently, security is a kind of service that needs a large amount of investment. Thus, it is impossible to provide the total security service without any charging. Service providers should find efficient methods to present strong security service as value-added service.

- *Various secure algorithms and protocols in different types of terminals*

  A variety of security algorithms and protocols exists in different types of terminals. A rigorous problem is how to organize them to provide not only enough security, but also full interoperation among different types of mobile terminals. The problem cannot be solved without an effective security policy. Since a general mobile network includes various types of terminals, it is necessary to develop a security policy at both the terminal and network ends that can satisfy the security requirements effectively.

- *Different security requirements for various users and applications*

  Although secure communication is important in many applications, such as e-commerce, etc., many other applications require just a low level of security, such as accessing the Internet for open information. In this case, the unidirectional authentication from network to user may be enough. Therefore, security requirements vary among different users and services. Service providers should provide differentiated security services to users. The structure of security policy is necessary to provide the differentiated security. By this means, it is important to study the differentiated security service that is driven by security policy.

- *Simple and effective security services for users*

  Security management is of critical importance in network security. For example, a network is totally unsecured without effective security management even though it deploys many advantageous security entities and implements perfect security solutions. A secure network not only requires professional security managers at the network end, but also mobile users who can take charge of security management at the terminal end. If security management fails at either end, communication is unsecure. As we know, it is impossible to require that all users have enough security management ability. Thus, for better services, it is necessary to develop an effective security policy that is as simple as possible at the terminal end, and in which most policy decisions are executed in the network. For some services, all of the security policies may be determined at the (network) server end, such as e-banking services, etc.

Recommendation ITU-T X.1123

Differentiated security service for secure mobile end-to-end data communication

1 Scope

This Recommendation provides a specification of differentiated security services for secure mobile end-to-end data communication, which includes a series of security policies, security levels and negotiation of security levels between security domains.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control: [ITU-T X.800].

3.1.2 anonymity: [ITU-T X.1121].

3.1.3 application server: [ITU-T X.1121].

3.1.4 application service: [ITU-T X.1121].

3.1.5 application service provider (ASP): [ITU-T X.1121].

3.1.6 authentication: [ITU-T X.800].

3.1.7 authentication exchange: [ITU-T X.800].

3.1.8 authorization: [ITU-T X.800].

3.1.9 availability: [ITU-T X.800].

3.1.10 confidentiality: [ITU-T X.800].

3.1.11 data integrity: [ITU-T X.800].

3.1.12 encipherment: [ITU-T X.800].

3.1.13 identity management: [ITU-T X.1121].

3.1.14 integrity: [ITU-T X.800].

3.1.15 key: [ITU-T X.800].

3.1.16 mobile network: [ITU-T X.1121].

3.1.17 mobile terminal: [ITU-T X.1121].

3.1.18 mobile user: [ITU-T X.1121].

3.1.19 non-repudiation: [ITU-T X.800].

3.1.20 password: [ITU-T X.800].

3.1.21 privacy: [ITU-T X.800].

3.1.22 security dimension: [ITU-T X.805].

3.1.23 security policy: [ITU-T X.800].

3.1.24 usability: [ITU-T X.1121].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security level: Security level is the application of a network system to process information with different sensitivities and to permit simultaneous access by users with different security clearances and needs-to-know.

3.2.2 security policy server: A security policy server is an entity that connects to a security gateway. It manages security policy and uses the security policy to control the negotiation of security levels among network security domains.

3.2.3 service provider: A service provider is a business that provides service to customers over a network; it includes not only network service providers but also application service providers.

3.2.4 assets: Assets are valuable properties to be protected by the mobile terminal or service provider. Assets are divided into three kinds: information, service, and system assets.

3.2.5 security manager: A security manager is a person or entity that determines the security service level, manages the configuration of security policy, and performs security policy-related tasks at the mobile terminal or service provider.

3.2.6 security service: A security service is a service provided by the service provider to ensure adequate security of the systems or of data transfers. It includes not only eight security dimensions, but also online virus scanning and content filtering.

3.2.7 differentiated security service: A differentiated security service is a security service with a security policy that classifies different security levels.

3.2.8 security gateway: A security gateway is an entity which relays data traffic between security domains, configures security parameters or communication protocols and can perform a security policy management function.

3.2.9 user security agent: A user security agent is an entity embedded in mobile terminals to collect the security-related environmental information and to communicate with the security gateway in the mobile network for the execution of the security policy.

3.2.10 security domain: A security domain is a set of dimensions, a security policy, a security authority and a set of security-related activities in which the set of dimensions is subject to the security policy for the specified activities, and whereby the security authority administers the security policy. It is a collection of users and systems subject to a common security policy.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AKA	Authentication Key Agreement
ASP	Application Service Provider
CNP	Client-to-Network Protocol
GCI	Gateway Communication Interface
GSSAI	Generation of Security Service accounting Information
MSL	Management of Security Level
MUI	Management of User Information
NNP	Network-to-Network Protocol
NSP	Network-to-Server Protocol
SCI	Server Communication Interface
SGW	Security Gateway
SLN	Security Level Negotiation
SPS	Security Policy Server
SSCU	Security Service Control Unit
UCI	User Communication Interface
ULS	User Level Set
USA	User Security Agent

5 Conventions

None.

6 Network model for differentiated security service

Before describing secure mobile technologies, a network model for differentiated security service should be defined. It describes the communication among the different security entities.

Network security is always based on security domains. For mobile networks, it can be divided into two types of security domains. One is the access network security domain, and the other is the core network security domain. A communication from sender to receiver always crosses three security domains, i.e., the access network security domain at the sender end, the core network security domain and the access network security domain at the receiver end. The security gateway (SGW) is located at the edge of security domains and interconnects two security domains. Security mechanisms are always installed in the SGW. Mobile terminals can also be considered to be a type of SGW because they are also located at the edge of the security domain and install security functions.

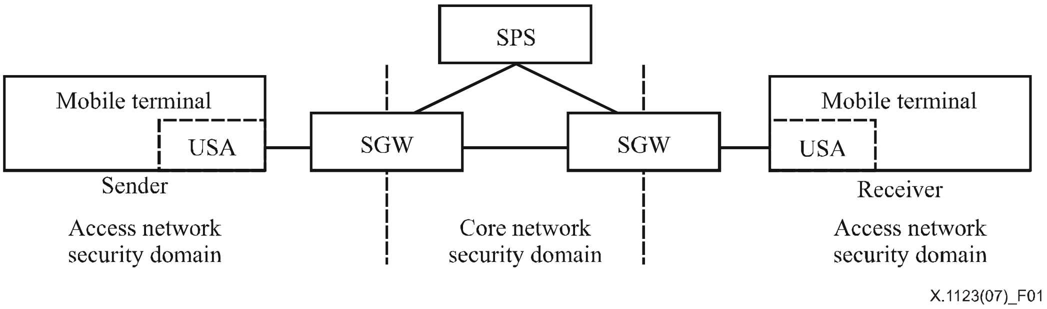

SPS
Mobile terminal
USA
SGW
SGW
Mobile terminal
USA
Sender
Receiver
Access network security domain
Core network security domain
Access network security domain
X.1123(07)_F01

Figure 1 – Network model for differentiated security service

A network model for differentiated security service is shown in Figure 1. A communication path between the sender and receiver is set up by SGW, which negotiates security parameters and triggers security resources to safeguard communication across the security domains. The security policy server (SPS) controls the security service.

This network model also supports the scenarios, where the receiver is an application server, such as where mobile terminals access bank services. In this way, SPS is integrated into the application server. Thus, communication from sender to receiver may cross only two security domains, the access network security domain at the sender end and the core network security domain at the receiver end.

7 Differentiated security service

7.1 Types of assets in the mobile environment

The security in the mobile environment protects the assets from the attacker. The assets may be identified in both the mobile terminal and the SGW at the edge of security domains, which are protected by differentiated security levels agreed by the two corresponding entities via an in-band channel or out-of-band channel, respectively.

Assets are defined as valuable properties that should be protected in transmission. In order to negotiate the security policy between the mobile terminal and the SGW, assets should be identified and protected by security mechanisms. Assets in the mobile communication context can be grouped into three types: information assets, system assets, and service assets. System assets and service assets are of a static nature, as these assets would usually remain unchanged after setting up. However, information assets are dynamically managed assets, because they are created, removed, modified or deleted according to the policy of the mobile terminal or the application service provider (ASP). Information assets could be stored in system assets and could be manipulated by service assets. Service assets can be created, deleted or managed by using system assets. Table 1 describes assets with examples. These three types of asset should be protected according to the appropriate security policy negotiated or pre-agreed between the mobile terminals or between the terminal and the ASP. This Recommendation only focuses on information assets.

Table 1 – Classification of assets

Class	Description	Example
Information asset	Valuable data that can be stored, processed or transferred by computational systems.	Sensitive data, E-transaction data, Business plan
Service asset	Application program that offers the manipulation of data to users.	Web service E-mail service
System asset	Physical hardware components for supporting services and data processing.	File server Telnet server

7.2 Framework of differentiated security service

Differentiated security services are driven by security policy. Security policy is divided into various security layers and then every security layer may be divided into several security levels. The security level is assigned to assets that are protected by our model. It is necessary to establish the security policy for the context of both access network security domains and core network security domains, to apply them to all kinds of assets: service assets, system assets, and information assets. If the security policy is negotiated online, the integrity and authenticity of security policy sent from one terminal to another should be assured via some security mechanisms: digital signature, message authentication code and pre-shared secret.

Operators should set up classification of security policy, its corresponding amount of security layers and security levels in every layer. Figure 2 proposes a typical example to illustrate the framework of differentiated security service. The corresponding security policy is divided into three security policy layers, which consist of super security policy, baseline security policy and no security policy. Again, the super security policy layer can be divided into several levels. However, the number of security levels should depend on the configuration from operators. In order to meet the security requirements from various scenarios, it is preferable to allow both the mobile terminal and the SGW to set up the acceptable security policies, including the number of security layers and security levels.

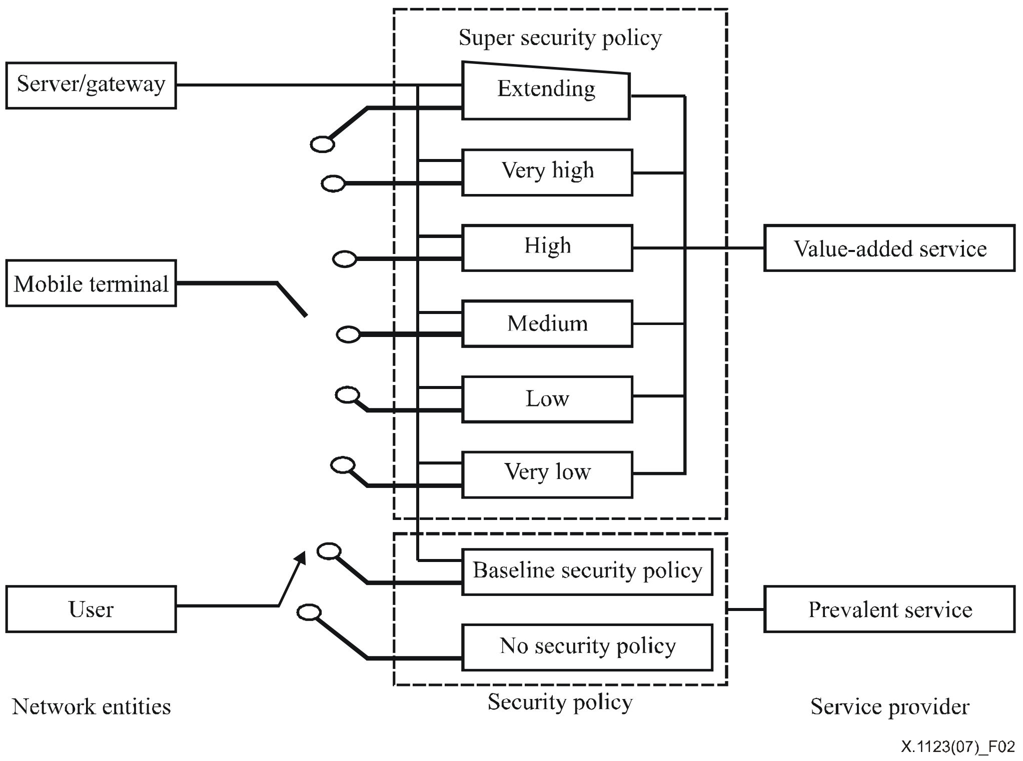


Figure 2 – Framework of differentiated security service

There are three parts in the illustration of the framework of differentiated security service. The first part is network entities involving SGW, user security agent and user. The second part, named security policy, is divided into three layers: super security policy, baseline security policy and no security policy. The third part is ASP that provides two types of security services. The first type is the prevalent service for baseline security policy and no security policy. The second type is value-added service for super security policy.

- *SGW*

  SGW is very important for mobile communication that supports both baseline policy and super security policy.

- *Mobile terminal*

  Only one of the security levels is available for a communication process among no security policy, baseline security policy, very low super security policy, low super security policy, medium super security policy, high super security policy, very high super security policy and extending super security policy and baseline security policy.

- *User*

  Select a security policy in the mobile terminal for a communication process according to the value of information asset that will be transferred.

7.2.1 No security policy as prevalent service

No security policy is defined as the policy under which the mobile terminal and SGW do not trigger security-related functions.

Some applications may not require any security functions in the transport stratum. The security of communication with no security policy may depend on the security that is provided by an upper layer. But it is recommended that at least baseline security policy should be assigned in the transport stratum in order to provide basic communication security.

7.2.2 Baseline security policy as prevalent service

Baseline security policy is required for all data communication. Thus, it can be considered as a prevalent service that the ASP provides. The mobile network should support the baseline security policy that cannot be disabled by either the user or the ASP. It mainly provides enough protection for accounting. Users can use the baseline security policy to get open data information from servers.

According to the security requirements from both the user's and ASP's points of view that are discussed in [ITU-T X.1121], some belong to the requirements that the baseline security policy should realize. These are listed as follows:

- unidirectional authentication;
- identity management;
- usability;
- availability.

In order to process accounting, unidirectional authentication processes are provided from the server to the mobile terminal and from the mobile terminal to the user. Accounting is a basic requirement of the ASP. On the other hand, identity management is necessary for authentication.

7.2.3 Super security policy as value-added service

Except for the security requirements for the baseline security policy, all other security requirements should belong to the super security policy provided as a value-added service. The security requirements include, but are not limited to:

- authentication;
- confidentiality;
- integrity;
- anonymity;
- access control;
- non-repudiation;
- privacy.

Operators should define several security levels for the super security policy layer, especially for terminals with limited computing power. Users can easily select suitable security levels according to the importance of interactive data before communication begins. In the super security policy layer, different security levels may correspond to different prices of the security service.

Mobile terminals should at least support the following security levels listed as follows:

- very high;
- high;
- medium;
- low;
- very low;
- extending.

The level of "very high" is the highest security that can be provided to the users. Entities can use stronger cryptogram algorithms and longer key length to achieve it. It always consumes much more computing power on both the terminal device and the SGW. Thus the service price of "very high" security should be the highest. On the contrary, "very low" level indicates that the data communication is only protected weakly. The "extending level" describes the security enforcement that can be combined agilely.

Table 2 presents a description of criteria for assigning security levels to each security domain and asset. The super security policy layer can be classified as five levels, i.e., very high, high, medium, low and very low. These security levels could be assigned according to policy by the mobile terminal and the SGW. As it is too complex and difficult to make a unified and unique security level, careful investigation is required to determine the appropriate security policy. Therefore, a typical example of criteria to assign the security level to assets is very useful for the security manager.

Table 2 – Criteria for assigning security levels to assets

Grade	Security level for security domain	Sensitivity level (for asset)
Very high (+2)	There exists a documented organization security policy. Appropriate security measures are applied to the organization's network. Incident response process is prepared. Regular security monitoring is performed.	If the asset is destroyed, forged or exposed, it will cause a long-term discontinuity of the organization's task. If the asset is damaged, it cannot be recovered.
High (+1)	There exists a documented organization security policy. Appropriate security measures are provided against known attacks. Regular security monitoring is being performed.	If the asset is destroyed, forged or exposed, it will cause a short-term discontinuity of the organization's task. If the asset is damaged, it can be recovered.
Medium (0)	Appropriate security measures are applied against known attacks. Regular security monitoring is being performed.	If the asset is destroyed, forged or exposed, it will cause temporary inconvenience to the organization's task. If the asset is damaged, it can be recovered.
Low (–1)	Appropriate security measures are applied against known attacks. Irregular security monitoring is being performed.	Although the asset is destroyed, forged or exposed, there will be little effect on the organization's task. If the asset is damaged, it can be recovered.
Very low (–2)	There exist no security measures.	Although the asset is destroyed, forged or exposed, there will be no effect on the organization's task.

ASPs can configure security technology used at every level as the market requires. Moreover, with the development of security technology and different types of terminals, the technical content in a level may be different for the time being. However, the definition of levels according to the strength of security can give users a uniform and stable solution to enjoy secure service. Users need not know the detailed security technology used at every level. They care only about the relationship between the different service scenarios and the different security levels. Before the establishment of data communication, users need only make simple judgements and decisions. For example, they can simply use the baseline security policy with which they need not make any selection. They can also select one of the higher security levels to communicate according to the importance of data.

8 Security policy

The criteria of security policies are driven by security requirements, and should be adhered to by network entities. There are three basic requirements involving completeness, correctness and consistency. Firstly, the defined policy should protect the targets defined within different kinds of security requirements; secondly, the defined policy should be practicable, namely, it does not diminish over time; thirdly, there should not be any conflicting policies that may result in variable decisions when applied to mobile communication.

The security policy is divided into several security levels. A security layer can be considered as one group of security levels. Each level provides a different strength of security for the service. The security manager can produce rules on the classification of security levels.

8.1 Framework of security policy

Security policy is composed of four factors: security levels, security scenarios, security dimensions, and security algorithms and protocols. As shown in Figure 3, the security algorithm and protocol can be determined by the security level, the security scenario and security dimension together.

Security dimension 1

	High	Medium	Low	Extending
Security scenario 1	Algorithm 1.1.1 and protocol 1.1.1	Algorithm 1.1.2 and protocol 1.1.2	Algorithm 1.1.3 and protocol 1.1.3	Algorithm 1.1.4 and protocol 1.1.4
Security scenario 2	……	……	……	……
……	……	……	……	……
Security scenario n	Algorithm 1.n.1 and protocol 1.n.1	Algorithm 1.n.2 and protocol 1.n.2	Algorithm 1.n.3 and protocol 1.n.3	Algorithm 1.n.4 and protocol 1.n.4

Security dimension i

	High	Medium	Low	Extending
Security scenario 1	Algorithm i.1.1 and protocol i.1.1	Algorithm i.1.2 and protocol i.1.2	Algorithm i.1.3 and protocol i.1.3	Algorithm i.1.4 and protocol i.1.4
Security scenario 2	……	……	……	……
……	……	……	……	……
Security scenario n	Algorithm i.n.1 and protocol i.n.1	Algorithm i.n.2 and protocol i.n.2	Algorithm i.n.3 and protocol i.n.3	Algorithm i.n.4 and protocol i.n.4

Figure 3 – Framework of security policy

8.1.1 Security level

Classification of the security level is performed by the security manager based on the security requirement as required by the market. For example, security policy can be simply divided into three levels of high, medium and low. If necessary, it can also be divided into more levels. Different security levels provide users with different security services. Thus, users can choose a specific security level according to their security requirements.

The same security level for different services may represent different definitions, including different algorithms and/or different protocols. For example, the high security level for mobile payment services may use complicated authentication, authorization, encryption, signature, etc.; however, the high security level of presence may not include the signature function and related-security protocols.

8.1.2 Security scenario

The security scenario is another factor of security policy. A security scenario corresponds to a style of services that have the same operational processes. According to the security requirement, the security manager combines different operational processes into one unit scenario, which is transparent to users. For example, both mobile e-banking and mobile insurance require high confidentiality of communication, so they belong to one security scenario.

8.1.3 Security dimension

As the third factor of security policy, a security dimension is the functional unit that implements security services. A security dimension is a counter-measure against certain security threats. All of the security dimensions are taken into account for the main security threats. [ITU-T X.805] identifies eight dimensions that protect against all major security threats, including access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy. Moreover, the security dimension can also include online anti-virus, intrusion detection, content filtering and vulnerability scan.

8.1.4 Security algorithm and protocol

The last factor of security policy relates to detailed protocols and algorithms. Each security dimension is realized with certain kinds of algorithms and protocols. That is, security mechanisms for every security dimension will be defined. Mobile terminals and security gateways may support different algorithms and protocols. They should share some common information on the identifiers of supported algorithms and protocols. As shown in Figure 3, each security dimension has one table. Each table is divided into a different collection of algorithms and protocols based on the security level and security scenario. In the table of one security dimension, a certain security level and security scenario determine the security algorithm and protocol of its dimension. Algorithms and protocols of different security dimensions together protect the communication under the particular security scenario and security level. For example, under the condition of medium security level and security scenario 1, if security dimension 1 and security dimension 3 are included to protect the communication, algorithm 1.1.2/protocol 1.1.2 and algorithm 3.1.2/protocol 3.1.2 will be used in this communication.

8.2 Configuration of security policy

The content is divided into four aspects that are used to configure the different security levels. They include:

- lists of identifiers for security level;
- lists of identifiers for security scenario;
- lists of identifiers for security dimensions;
- lists of identifiers for security algorithms and protocols.

In practice, the security policy is placed in the SPS and then downloaded to the SGW and mobile terminal. Considering that one SGW may connect with more than one mobile terminal and one SPS may connect with more than one SGW, the security policy used by the SGW is a subset of that in the SPS. The security policy used by the mobile terminal is a subset of that in the security gateway. The SGW and mobile terminal can download a subset of a security policy or simply download the whole of a security policy from the SPS. This depends on which method is easier to implement and more economical in practice.

9 Negotiation process

The mobile terminal and SGW may negotiate the security policy either online or out-of-band because the differentiated security service depends on the security policy in the mobile terminal and ASP.

Security policy management between the mobile terminal and the SGW is asymmetric. The negotiation between them is not a peer-to-peer process.

At the mobile terminal, the user can configure security policy manually. For example, the user can simply select one item from among high, medium and low as needed to finish the security policy configuration for a particular service.

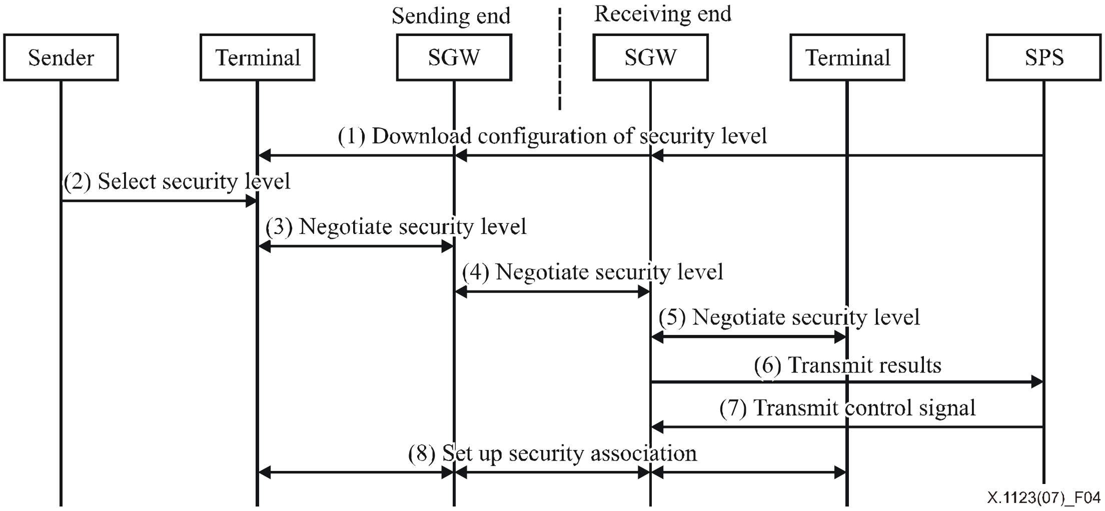
However, it is necessary to add an SPS to execute complex security management at the SGW. The SPS should analyse the security technology from the mobile terminal and try to understand the security protocols that the mobile terminal supports. It should also evaluate the level of security with different compositions of security protocols. The SPS can decide from acceptance, rejection and conditional acceptance of the communication. Detailed rules for conditional acceptance can be configured in the SGW.

Negotiation is performed between the mobile terminal and SGW for parameters relating to security dimensions, including security algorithms and protocols. If security levels are different between a user's selection and the result of negotiation, the security level from the result of negotiation should be higher than that from the user's selection.

9.1 Negotiation process of security policy

The negotiation of security policy comprises two types, a static process and a dynamic process. When the user need not select the security level that is determined by the SPS, it is a static process. On the other hand, when the security level of an application should be selected by users, it is a dynamic process.

The security level in a static process always binds with one type of service. A single security level is enough to meet the security requirements of that service. For example, the security level for e-banking services always requires the highest degree of security. Thus, all the activities of e-banking services are bound to the highest security level. Users need not make any selection.



Sending end
Receiving end
Sender
Terminal
SGW
SGW
Terminal
SPS
(1) Download configuration of security level
(2) Select security level
(3) Negotiate security level
(4) Negotiate security level
(5) Negotiate security level
(6) Transmit results
(7) Transmit control signal
(8) Set up security association
X.1123(07)_F04

Figure 4 – Negotiation process of security policy

The SPS can classify security into several levels. According to the security requirements, it generates a security policy to regulate the differentiated security levels and store them on the SPS. Negotiation is carried out hop-by-hop, i.e., from one security domain to the other. This is shown in Figure 4 and their processes in detail are listed as follows:

1) As it provides security service for the first time, the SGW downloads or refreshes security level configurations from the SPS, and then the terminals will download the security level configurations from the SGW.

2) The sender selects a security level according to the application scenario of the current service.

3) Security level negotiation is carried out between the terminal and the SGW at the sending end. If the negotiation succeeds, proceed to step (4); otherwise, stop the negotiation. The detailed process is stated in clause 9.2.

4) Negotiation is carried out between the SGW at the sending end and the receiving end. If the negotiation succeeds, proceed to step (5); otherwise, stop the negotiation. The detailed process is stated in clause 9.3.

5) Negotiation is carried out between the SGW and the terminal at the receiving end. If the negotiation succeeds, proceed to step (6); otherwise, stop the negotiation. The detailed process is stated in clause 9.4.

6) The SGW at the receiving end transmits the negotiation result of (5) to the SPS. The SPS makes a decision (accept or reject) according to the negotiation result.

7) The SPS transmits a decision to the SGW at the receiving end. If the decision is acceptable, then proceed to (8); otherwise, stop the negotiation.

8) The security association at a particular security level is set up between the terminal and the SGW at the sending end, between the SGW of the sending end and the receiving end, and between the SGW and the terminal at the receiving end.

Steps (3), (4) and (5) show three types of the negotiation processes. The first is negotiation between the terminal and the SGW at the sending end; the second is between two SGWs at both the sending and the receiving end; the third is between the SGW and the terminal at the receiving end.

9.2 Negotiation process between terminal and SGW

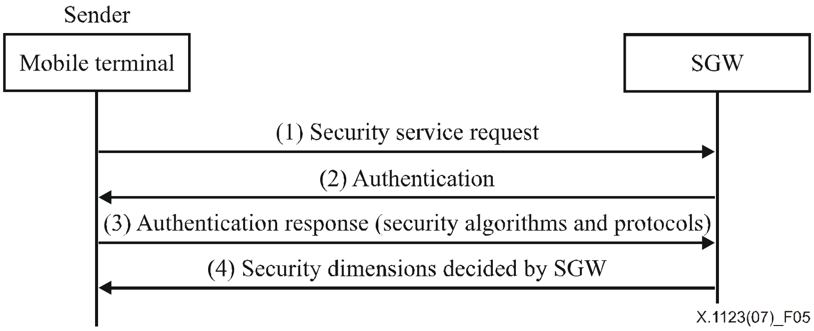

Sender
Mobile terminal
SGW
(1) Security service request
(2) Authentication
(3) Authentication response (security algorithms and protocols)
(4) Security dimensions decided by SGW
X.1123(07)_F05

Figure 5 – Negotiation of security policy at the sending end

The negotiation process between the terminal and the SGW at the sending end consists of the following four steps:

1) The terminal sends a security service request message to the SGW.

2) The SGW sends an authentication challenge to the sender by using an authentication vector, which is used to authenticate and negotiate session keys with the sender. The SGW uses the session keys (encryption key and integrity key) to protect this message.

3) The terminal authenticates the SGW. After successful authentication, the terminal computes the session keys, then sends the following information to the SGW under the integrity protection using the agreed integrity key:

   a) An authentication response.

   b) A list of identifiers for integrity and encryption algorithms, which are supported by the sender.

   The negotiation procedure is aborted if authentication or integrity check fails.

4) The SGW authenticates the terminal. If authentication is successful, the SGW sends an identifier that is decided by the security policy. This message is protected by the integrity using the agreed integrity key. The negotiation procedure is aborted if authentication of the SGW to the sender or the integrity check on message fails.

In the negotiation procedure, the SGW needs an authentication vector to protect the message before establishing a secure channel. There are encryption keys and integration keys in the authentication vector, while the mobile terminal can calculate the two keys through authenticate challenge. Detailed information can be found in 3GPP AKA mechanism [b-3GPP TS 33.102].

9.3 Negotiation process between SGWs

The security negotiation process is always time consuming. In order to improve the efficiency of the negotiation process, predetermined fixed (relative high) security levels can be adopted in the core network security domain. Because the status of security requirements in the core security domain is always stable, it is preferable to use fixed security levels between the SGWs.

9.4 Negotiation process between SGW and terminal

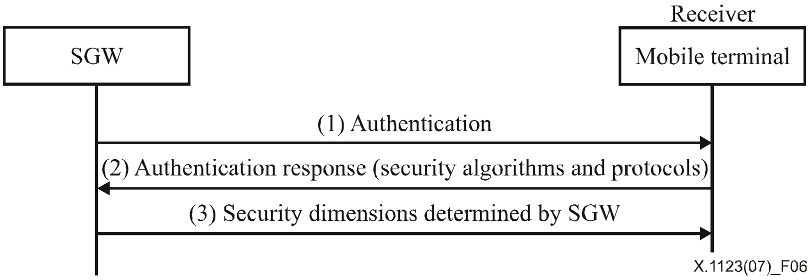

Receiver
SGW
Mobile terminal
(1) Authentication
(2) Authentication response (security algorithms and protocols)
(3) Security dimensions determined by SGW
X.1123(07)_F06

Figure 6 – Negotiation of security policy at the receiving end

The negotiation process between the SGW and the terminal consists of the following three steps:

1) The SGW sends the chosen security algorithms and protocols, and the authentication challenge to the terminal. The authentication challenge uses an authentication vector, which is used to authenticate and negotiate the keys with the receiver. The SGW uses session keys (encryption key and integrated key) to protect this message.

2) The terminal authenticates the SGW. After a successful authentication, the terminal computes the session keys, sends an authentication response and negotiation response to the SGW. The terminal uses the session keys to protect the message. The negotiation procedure is aborted if the authentication or integrated checking fail.

3) The SGW authenticates the terminal. If authentication is successful, the SGW and the terminal establish a secure channel according to the chosen security algorithms. The negotiation procedure is aborted if the authentication or integrated check fail.

In the negotiation procedure, the SGW needs the authentication vector to protect the message before establishing a secure channel. There are encryption keys and integration keys in the authentication vector, while the mobile terminal can calculate the two keys through the authenticate challenge. Detailed information can be found in [b-3GPP TS 33.102].

10 Billing of security service

SGW collects accounting information and sends them to the billing centre. Such information includes starting/ending time of communication, volume of information transmitted, and the count of the number of invocations of a security service.

Accounting information related to the usage of a security service can be transformed into a format that can be recognized by the billing centre. The SGW collects accounting information and transmits it to billing centre. The SGW mainly performs the following functions:

- Decompose comprehensive accounting information related to the usage of the security service according to the billing method used by the operator. Methods involve basic billing modes, such as a) by number of invocations of a security service; b) by volume of information transmitted; and c) by duration of communication.
- Generate basic records for billing events, according to the different types of accounting information identified above.
  a) For billing based upon number of invocations, the event record contains the number of times that the security service was invoked, and the identification of the service.
  b) For billing based upon volume of data transmitted, the event record contains volume of information transmitted, and the identification of the service.
  c) For billing based upon duration of communication, the event record contains starting and ending times of communication, and the identification of the service.

11 Triggering of security resources

Security resources in entities should be triggered by security policy. The security policy is managed and distributed by the SPS. Therefore, the SPS controls the running of security resources. For example, authentication, encryption and digital signature may be triggered according to the selected security level.

Annex A

Functions of the network model for differentiated security service

(This annex forms an integral part of this Recommendation)

A.1 Functions of the network model

The network model for the differentiated security service is shown in Figure 1. The communication channel between the sender and the receiver is set up by the SGW, which negotiates and triggers security algorithms and protocols to safeguard communication section by section. The SPS controls the differentiated security service.

Figure A.1 shows the functions of Figure 1. The function of each network entity is divided into several modules. More detailed specifications are described below.

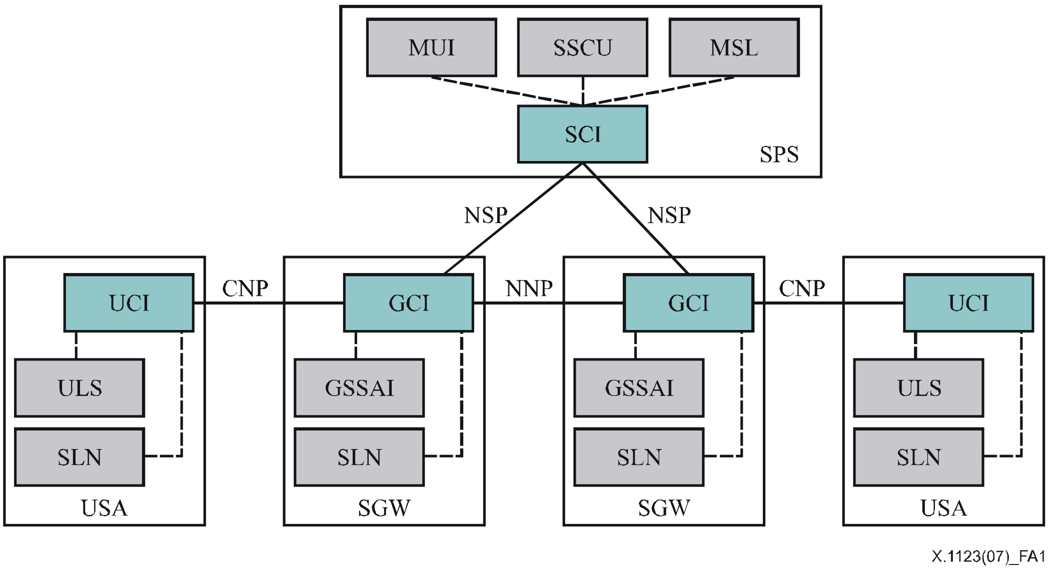


Figure A.1 – Functions of reference model for differentiated security service

A.2 Depiction of functions

A.2.1 USA

The USA renews the policy of security levels from the SGW once they have been changed in the SPS. Once the user chooses a particular security level for one service, the USA sends the selection to the SGW. Both sender and receiver can choose the appropriate security level for the service. Depending on the security levels supported by the sender, receiver and SGW, the USA will negotiate the final security level with the other network entities. The USA can also upload the update of user information to the SGW.

A.2.1.1 Module functions

- *User communication interface (UCI)*

  This module is responsible for communicating with the GCI of the SGW. The UCI collects and uploads user information to the GCI and renews the policy of security levels, billing information, etc.

- *Security level negotiation (SLN)*

  The SLN sets up, maintains and releases the security communication channel from the sender to the receiver after the negotiation between the USA and the SGW is finished. The chosen security level must be not lower than the security level requested by the sender.

- *User level set (ULS)*

  The ULS stores the user's configuration that includes user ID, password, list of available security levels, expense ratio, etc.

A.2.1.2 Interfaces between modules

- *Interface between UCI and ULS*

  i) The ULS uploads user's configuration to the UCI.

  ii) The ULS downloads the information of security levels, expense ratio from the UCI.

- *Interface between UCI and SLN*

  i) When the USA acts as a sender, the SLN sends the selected security level to the UCI for negotiation.

  ii) When the USA acts as a receiver, the SLN receives the selected security level from UCI for determination.

- *Interface between ULS and SLN*

  i) The ULS sends the security level selected by the user to the SLN.

  ii) When the security levels selected by the sender (receiver) and the SGW are different, the SLN is responsible for the negotiation and sends the negotiation results to the ULS. The user can decide whether the results are accepted or not.

A.2.2 SGW

The SGW connects with the USA, the SPS, and other SGWs. It uploads the SPS with the user's information that is collected by the GCI, synchronizes the security policy with the SPS, and sends the policy of security levels to the USA. It can set up secure communication channels with other entities after negotiation is successful.

A.2.2.1 Module functions

- *Gateway communication interface (GCI)*

  This module is responsible for communicating with the UCI, SCI and other GCIs. The GCI sets up and maintains secure communication channels according to the chosen security levels. The GCI receives the user information from the USA, and relays it to the SPS. The GCI also downloads the security policy from the SPS, and sends it to the USA.

- *Security level negotiation (SLN)*

  The SLN sets, maintains and releases secure communication channels after negotiation with the USA and other SGWs.

- *Generation of security service accounting information (GSSAI)*

  The GSSAI generates the accounting information according to security levels. The accounting information may include the types of data discussed in clause 10.

A.2.2.2 Interfaces between modules

- *Interface between GCI and SLN*

  i) During negotiation, the SLN obtains the parameters of the security level from the GCI.

  ii) After negotiation of each phase, the SLN transfers the results to the GCI.

  iii) After negotiation, the SLN obtains the results from the GCI.

- *Interface between SLN and GSSAI*

  The GSSAI receives communication information from the SLN and generates the billing information discussed in clause 10.

- *Interface between GCI and GSSAI*

  The GSSAI transfers the billing information to the GCI.

A.2.3 Security policy server (SPS)

The SPS stores the policy of the security level configured by the administrator and the security levels customized by the users. The SPS also arbitrates the security level in the multi-phase negotiation.

A.2.3.1 Module functions

- *Server communication interface (SCI)*

  The SCI receives the user information from the SGW and sends the security policy to the SGW.

- *Management of security level (MSL)*

  The MSL provides the administrator with a management interface with information about which the administrator can configure and update the security policy in the SPS.

- *Security service control unit* (*SSCU*)

  The SSCU arbitrates and decides the final security level when network entities choose different levels.

- *Management of user information (MUI)*

  The MUI records the user information, such as security levels customized by users, user accounting information, etc. When changed, the new user information is stored in the MUI.

A.2.3.2 Interfaces between modules

- *Interface between SCI and MSL*

  i) The MSL transfers security policies to SCI.

  ii) The MSL transfers user information to SCI.

  iii) The MSL receives user information from SCI.

- *Interface between SCI and SSCU*

  When network entities select different security levels for communication, the SSCU transfers arbitration of security level information to the SCI.

- *Interface between MSL and SSCU*

  i) The SSCU obtains configuration of security policy from the MSL.

  ii) The MSL obtains arbitration of security level from the SSCU.

- *Interface between MSL and MUI*

  i) The MUI obtains definitions and descriptions of certain service from the MSL, such as service id, locations, etc. Generally, the transmission is required when the user selects, orders or changes the service.

  ii) The MSL obtains user information from the MUI.

A.3 Protocols between functions

A.3.1 Client-to-network protocol

The CNP provides an interface between the UCI and GCI. Functions include:

a) The terminal sends requests for a security service to the SGW. Under the security policy from the SPS, the SGW responds with information, such as permit or deny, to the terminal.

b) Upload user's information to the SGW. It includes the user's customization of service and updates.

c) The USA downloads security policy and expense ratio from the SGW.

d) The SGW collects information including security level, start and end times of security communication, count of the number of invocations of security services, the volume of information transmitted, etc., from other entities.

e) Set up, maintain and release security communication channels from sender to receiver.

A.3.2 Network-to-server protocol

The NSP provides an interface between the GCI and SCI. Functions include:

a) The SGW downloads security policy from the SPS.

b) The SGW downloads user information from the SPS.

c) The SGW uploads to the SPS the information from the USA. The information includes user's configuration, updates, etc.

A.3.3 Network-to-network protocol

This interface negotiates parameters of security level between SGWs.

Appendix I

Example of security mechanism in line with subgroup of security policy

(This appendix does not form an integral part of this Recommendation)

Key distribution/sharing is needed for data confidentiality and authentication. Table I.1 describes the typical security mechanisms corresponding to each security dimension. The list in the last column of Table I.1 is of little significance, that is, it is NOT a mandatory option, and it can be only used as a guideline for security managers to determine their own security policy. The other security algorithms with the equivalent cryptographic strength or key length are available only if they are one of the algorithms chosen by the security manager for a specified application. The security manager of the application service provider assigns the specific security mechanism of every security dimension.

Table I.1 – Typical security mechanisms corresponding to security dimension of security policy

Security dimension	Security mechanisms		Typical security algorithms
Data confidentiality	Encipherment/ decipherment	Very high	AES-256, RSA-2048
		High	–
		Medium	AES-128, RSA-1024
		Low	–
		Very low	DES-64
Data integrity	Hash function	Very high	SHA-384
		High	–
		Medium	SHA-160
		Low	–
		Very low	MD5-128
User authentication	Authentication exchange	Very high	Bilateral authentication with GQ-2048
		High	–
		Medium	Bilateral authentication with GQ-1024
		Low	–
		Very low	Bilateral authentication with GQ-512
Data origin/receipt authentication	MAC	Very high	MAC with SHA-384
		High	–
		Medium	MAC with SHA-160
		Low	–
		Very low	SHA-MD5-128
Non-repudiation	Digital signature	Very high	DSA-2048
		High	–
		Medium	DSA-1024
		Low	–
		Very low	DSA-512

Table I.1 – Typical security mechanisms corresponding to security dimension of security policy

Security dimension	Security mechanisms		Typical security algorithms
Key exchange	Key exchange protocol	Very high	DH-2048
		High	–
		Medium	DH-1024
		Low	–
		Very low	DH-512
Access control	Access control mechanism	Very high	PMI (privilege management infrastructure)
		High	–
		Medium	RBAC
		Low	–
		Very low	MAC

Bibliography

[b-3GPP TS 21.133] 3GPP TS 21.133 (2001), *3G Security; Security Threats and Requirements.* <http://www.3gpp.org/ftp/Specs/html-info/21133.htm>

[b-3GPP TS 33.102] 3GPP TS 33.102 (2005), *3G Security; Security architecture (Release 6).* <http://www.3gpp.org/ftp/specs/html-info/33102.htm>

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G Security; Access security for IP-based service (Release 6).* <http://www.3gpp.org/ftp/specs/html-info/33203.htm>

[b-IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).* <http://www.ietf.org/rfc/rfc3329.txt?number=3329>

[b-OMA WV-040] OMA Standard WV-040 V1.2 (2005), *WV-040 System Architecture Model*. <http://www.openmobilealliance.org/Technical/release_program/docs/IMPS/v1.2-20050125/OMA-IMPS-WV-Arch-V1_2-20050125-A.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009